Listing and Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Previously Presented) A method for managing access to a scrambled program, within a network comprising a first device interconnected to a second device, the method comprising:

(a) receiving said scrambled program in said first device, said scrambled program comprising a scrambled data component and a descrambling key;

(b) rebundling, in said first device, said descrambling key using a unique key associated with said first device;

(c) receiving, in said second device, said scrambled data component and said rebundled descrambling key;

(d) obtaining in said second device said descrambling key from said rebundled descrambling key; and

(e) descrambling, in said second device, said scrambled data component using said descrambling key.

2. (Previously Presented) The method of Claim 1 wherein said descrambling key is encrypted and the step of rebundling comprises:

(a) decrypting said encrypted descrambling key using a key associated with said scrambled program; and

(b) re-encrypting said descrambling key using said unique key associated with said first device to produce said rebundled descrambling key.

3. (Previously Presented) The method of Claim 2 wherein said unique key associated with said first device is a public key, said public key being located in said first device and a corresponding private key being located in said second device.

4. (Previously Presented) The method of Claim 2 wherein the step of rebundling is performed within a first smart card coupled to said first device and

the steps of obtaining and descrambling are performed within a second smart card coupled to said second device.

5. (Original) The method of Claim 1 further comprising the step of initializing said first device within said network.

6. (Previously Presented) The method of Claim 5 wherein the step of initializing comprises the step of receiving a public key from a conditional access provider, said step of receiving comprising authentication of said conditional access provider.

7. (Previously Presented) The method of Claim 5 wherein a public key is prestored in a smart card coupled to said first device or in said first device.

8. (Previously Presented) The method of Claim 1 wherein said descrambling key is encrypted using a private means if said scrambled program is received from pre-recorded media or protected by a private means if said scrambled program is received from a service provider.

9. (Previously Presented) A Presentation device for managing access to a scrambled program comprising:

(a) means for receiving, from a first device coupled to the presentation device via a local network, said scrambled program comprising a scrambled data component and a rebundled descrambling key encrypted using a key associated with the local network;

(b) a module for decrypting, in said presentation device, said rebundled descrambling key to generate said descrambling key;

(c) a module for descrambling, in said presentation device, said scrambled data component using said descrambling key to obtain a descrambled program; and

(d) means for presenting said descrambled program.

10. (Previously Presented) A method for managing access to a scrambled program received from a service provider within a network having an access device and a presentation device, said method comprising:

(a) receiving said scrambled program in an access device, said scrambled program comprising a scrambled data component and an encrypted descrambling key;

(b) decrypting, in said access device, said encrypted descrambling key using a key associated with said service provider;

(c) re-encrypting said descrambling key, in said access device, using a public key associated with said access device;

(d) receiving, in said presentation device, said scrambled data component and said re-encrypted descrambling key;

(e) decrypting, in said presentation device, said re-encrypted descrambling key to obtain said descrambling key; and

(f) descrambling, in said presentation device, said scrambled data component using said descrambling key.

11. (Previously Presented) The method of claim 9 wherein said scrambled program is prerecorded on media and provided to said access device, said encrypted scrambling key being received from said prerecorded media.

12. (Previously Presented) A method for recording a scrambled program received from a service provider, said method comprising:

(a) receiving said scrambled program in an access device, said scrambled program comprising a scrambled data component and an encrypted descrambling key;

(b) decrypting, in said access device, said encrypted descrambling key using a key associated with said service provider;

(c) re-encrypting said descrambling key, in said access device, using a public key associated with said access device;

(d) receiving, in a recording device, said scrambled data component and said re-encrypted descrambling key; and

(e) recording said scrambled data component and said re-encrypted descrambling key on media coupled to said recording device, and providing said scrambled data component and said re-encrypted descrambling key to a presentation device.

13. (Original) The method of Claim 12 wherein said scrambled program is prerecorded on media.

14. (Original) The method of claim 1, wherein the first device is an access device and wherein the second device is a presentation device.

15. (Previously Presented) A method for transforming in a security device, content information contained in a scrambled program received from a service provider comprising:

receiving in said security device the scrambled program containing scrambled content information and a descrambling key;

descrambling the scrambled content in the security device using the descrambling key;

generating in the security device another scrambling key;

re-scrambling the content using said another scrambling key; and

encrypting a local entitlement control message containing said another scrambling key using a unique key, and

providing said re-scrambled content and said local entitlement control message to a presentation device.

16. (Original) The method of claim 15, further comprising determining user entitlement to the scrambled program prior to descrambling the scrambled content.

17. (Previously Presented) An access device, comprising:

a signal input for receiving a scrambled program from a service provider, the scrambled program including a scrambled data component and an encrypted descrambling key;

a decrypting unit for obtaining the descrambling key using a key associated with the scrambled program;

an encryption unit for re-encrypting the descrambling key using a public key associated with the access device;

a signal output coupled to a digital bus for transmitting the scrambled data component and the re-encrypted descrambling key to a presentation device via the digital bus, wherein only a presentation device having a corresponding private key is able to decrypt the re-encrypted descrambling key and descramble the scrambled content.

18. (Previously Presented) The access device of claim 17, wherein the public key is periodically received from a conditional access provider.

19. (Previously Presented) The access device of claim 17, wherein the signal output authenticates the presentation device before transmitting the scrambled data component and the re-encrypted descrambling key to the presentation device.

20. (Previously Presented) The access device of claim 17, wherein the signal output transmits identification data associated with the access device and copy control information along with the re-encrypted descrambling key.